MAT205: Abstract Algebra II

Finite Simple Groups Through Three Examples

Ma, Jia-Jun - Xiamen University Malaysia

Goal

Lecture 8 ended with **composition factors**: every finite group breaks into a list of finite simple groups. So every finite group is "made of" simple groups.

This raises one natural question:

> Which finite simple groups are there?

The full answer is the **Classification of Finite Simple Groups** (CFSG), one of the deepest theorems of 20th-century mathematics. We will not prove it. Instead, we **meet three concrete examples**, one from each kind of family CFSG describes.

Topics

1. The landscape: what CFSG actually says.
2. **Example 1.** $\mathrm{PSL}_n(\mathbb{F}_p)$ – a classical Lie family.
3. **Example 2.** M_{12} – a sporadic group, via Steiner systems.
4. **Example 3.** G_2 – an exceptional Lie family, via octonions.
5. Looking back at the landscape; bridges to the next chapters.

Cast of Characters

Object	Role in this lecture
$\mathrm{PSL}_n(\mathbb{F}_p)$	Example 1 — a classical Lie family
Steiner system $S(5, 6, 12)$	the combinatorial object behind M_{12}
M_{12}	Example 2 — sporadic
Octonions $\mathbb{O}$	the algebra behind G_2
$G_2(\mathbb{F}_p)$	Example 3 — exceptional Lie type over $\mathbb{F}_p$

Part I

The Landscape of Finite Simple Groups

Recall

A group G is **simple** if its only normal subgroups are $\{1\}$ and G.

We have already met two infinite families of simple groups:

- L01: abelian simple groups are exactly $\mathbb{Z}_p$, p prime.
- L04: A_n is simple for $n \geq 5$.

Are there any others? The answer turns out to be: **yes, but only finitely many more "kinds".**

CFSG (≈ 2004)

Theorem (Classification of Finite Simple Groups). Every finite simple group is one of:

1. cyclic of prime order;
2. alternating A_n, $n \geq 5$;
3. of **Lie type**, split into:
   - **classical**: PSL, PSU, PSp, $\mathrm{P}\Omega^{\pm}$ over finite fields;
   - **exceptional**: G_2, F_4, E_6, E_7, E_8 and their twisted forms;
4. one of 26 **sporadic** groups.

The proof spans roughly $10\,000$ pages. We will not enter it. Instead, the rest of today is **three concrete examples**.

Today's Three Examples

We already know the first two families ($\mathbb{Z}_p$, A_n). The remaining two — Lie type and sporadic — are best learned by meeting examples.

Family	Today's example	Built from
classical Lie	$\mathrm{PSL}_n(\mathbb{F}_p)$	linear algebra over $\mathbb{F}_p$
sporadic	M_{12}	a Steiner system $S(5, 6, 12)$
exceptional Lie	$G_2(\mathbb{F}_p)$	the octonion algebra $\mathbb{O}$

Each example is built from a different mathematical object. Together they show how rich the answer to "which simple groups exist?" really is.

Part II

Example 1 – $\mathrm{PSL}_n(\mathbb{F}_p)$ (classical Lie type)

Linear Groups over $\mathbb{F}_p$

This first example you already know – we collect the orders in one place before extending the pattern.

By counting ordered bases of $\mathbb{F}_p^n$:

$$|\operatorname{GL}_n(\mathbb{F}_p)| = \prod_{i=0}^{n-1}(p^n - p^i).$$

The determinant map $\operatorname{GL}_n \to \mathbb{F}_p^\times$ is surjective:

$$|\operatorname{SL}_n(\mathbb{F}_p)| = \frac{|\operatorname{GL}_n(\mathbb{F}_p)|}{p-1}.$$

$$|\operatorname{PSL}_n(\mathbb{F}_p)| = \frac{|\operatorname{SL}_n(\mathbb{F}_p)|}{\gcd(n, p-1)}.$$

Simplicity of $\mathrm{PSL}_n(\mathbb{F}_p)$

Theorem (Jordan, Dickson). $\mathrm{PSL}_n(\mathbb{F}_p)$ is simple **except** in two small cases:

$$\mathrm{PSL}_2(\mathbb{F}_2) \cong S_3, \qquad \mathrm{PSL}_2(\mathbb{F}_3) \cong A_4.$$

Both are solvable, hence not simple.

For all other (n, p): $\mathrm{PSL}_n(\mathbb{F}_p)$ is simple.

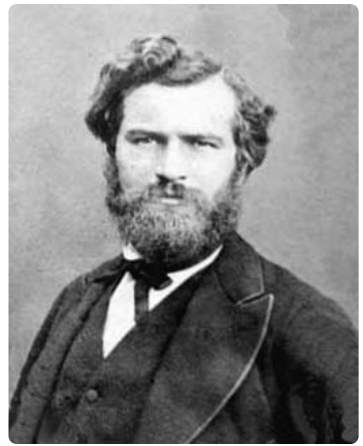
Foreshadowing: $G_2(\mathbb{F}_2)$ is also non-simple – same small-characteristic flavour.

Camille Jordan (1838–1922)

French mathematician. His *Traité des substitutions et des équations algébriques* (1870) was the first systematic textbook on group theory after Galois — and the first complete treatment of permutation groups, k-transitivity, and what we now call simple and solvable groups.

In the same volume Jordan proved the simplicity of $\mathrm{PSL}_2(\mathbb{F}_p)$ for $p \geq 5$, the case $n = 2$ of the theorem we just quoted.

His name is also attached to the Jordan curve theorem, Jordan canonical form, and (jointly with Hölder) the Jordan–Hölder theorem we used in L08.



C. Jordan (1838–1922)

Leonard Eugene Dickson (1874–1954)

American algebraist; first PhD in mathematics at the University of Chicago (1896). His book *Linear Groups, with an Exposition of the Galois Field Theory* (1901) was the first systematic treatment of the finite linear groups $\mathrm{GL}_n(\mathbb{F}_q)$, $\mathrm{PSL}_n(\mathbb{F}_q)$ and their simplicity.

Dickson completed the simplicity theorem for $\mathrm{PSL}_n(\mathbb{F}_q)$ in arbitrary n and q, extending Jordan's $n = 2$ case.

In 1905 he constructed the finite groups of type G_2 and proved their simplicity – we will return to this when we discuss $G_2(\mathbb{F}_p)$ in Part IV.

L. E. Dickson (1874–1954)

Beautiful Coincidences

Group	Order	Isomorphism
$\mathrm{PSL}_2(\mathbb{F}_5)$	60	A_5
$\mathrm{PSL}_2(\mathbb{F}_7)$	168	$\mathrm{GL}_3(\mathbb{F}_2)$
$\mathrm{PSL}_2(\mathbb{F}_9)$	360	A_6
$\mathrm{PSL}_4(\mathbb{F}_2)$	$20\,160$	A_8

These are the only "exceptional isomorphisms" between alternating and PSL groups.

After them, the two families part ways forever.

Summary of Example 1

$\mathrm{PSL}_n(\mathbb{F}_p)$ gives an **infinite family** of finite simple groups, parametrised by (n, p).

Together with A_n, this is the second infinite family we know.

What the family looks like:

- a uniform construction (linear algebra over $\mathbb{F}_p$),
- a clean order formula,
- a few small-(n, p) exceptions where simplicity fails.

This is the texture of **Lie-type** simple groups in general. Now we move to two examples that look completely different.

Part III

Example 2 – Mathieu's M_{12} (sporadic)

Sporadic Simple Groups

Two waves of discovery, separated by a century:

- **1861**, Émile Mathieu: the five Mathieu groups $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$.
- **1965–1982**: 21 further sporadic groups discovered, ending with the **Monster** of order $\approx 8 \times 10^{53}$.

Total: 26 finite simple groups belonging to **none** of the four infinite families.

We focus on the smallest one with a clean construction: M_{12}.

Steiner Systems

To find a sporadic simple group, the strategy is: build a **rigid combinatorial structure**, then take its automorphism group.

Definition (Steiner, 1853). A **Steiner system** $S(t, k, v)$ consists of:

- a finite set X with $|X| = v$ (the **points**);
- a collection $\mathcal{B}$ of k-subsets of X (the **blocks**),

subject to one axiom:

$$\boxed{\text{every } t\text{-subset of } X \text{ is contained in } \textit{exactly one} \text{ block.}}$$

The condition "exactly one" is what makes the system rigid: the small parts (t-subsets) completely determine the larger parts (k-subsets) once the block collection is fixed.

How Many Blocks?

A Steiner system $S(t, k, v)$ has

$$|\mathcal{B}| = \frac{\binom{v}{t}}{\binom{k}{t}}$$

blocks.

Why. Count pairs (T, B) where T is a t-subset of X and B is a block containing T.

- Counting by T: each t-subset is in exactly one block, so the count is $\binom{v}{t}$.
- Counting by B: each k-block contains $\binom{k}{t}$ different t-subsets, so the count is $|\mathcal{B}| \cdot \binom{k}{t}$.

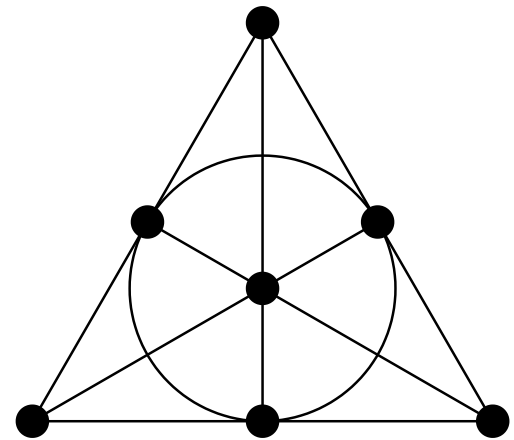
Equating gives the formula. So $\binom{k}{t}$ must divide $\binom{v}{t}$ for the system to exist – already a strong restriction on (t, k, v).

Example 1: $S(2,3,7)$ – the Fano Plane

- **Points.** $X = \{1,2,3,4,5,6,7\}$.
- **Blocks** (the "lines"):

$$\{1,2,3\},\ \{1,4,5\},\ \{1,6,7\},$$
$$\{2,4,6\},\ \{2,5,7\},$$
$$\{3,4,7\},\ \{3,5,6\}.$$

- **Block count check.** $\binom{7}{2}/\binom{3}{2} = 21/3 = 7$. ✓
- Every pair of points lies in **exactly one** line. This is the smallest projective plane.



$S(2,3,7)$ – the Fano plane

Fano Plane: Algebraic Interpretation

The Fano plane has a clean linear-algebra description over $\mathbb{F}_2$:

- **Points** $\longleftrightarrow$ nonzero vectors of $\mathbb{F}_2^3$ (there are $2^3 - 1 = 7$ of them);
- **Lines** $\longleftrightarrow$ 2-dimensional subspaces of $\mathbb{F}_2^3$, each containing 3 nonzero vectors.

So the Fano plane is the projective plane $\mathbb{P}^2(\mathbb{F}_2)$.

Group-theoretic version. Identifying $\mathbb{F}_2^3$ with the additive group $(\mathbb{Z}/2)^3$:

- the 7 points are the non-identity elements of $(\mathbb{Z}/2)^3$;
- the 7 lines are its 7 subgroups of order 4, each $\cong (\mathbb{Z}/2)^2$.

Automorphism group.

$$\mathrm{Aut}(\text{Fano plane}) = \mathrm{GL}_3(\mathbb{F}_2) \cong \mathrm{PSL}_2(\mathbb{F}_7), \qquad |\cdot| = 168,$$

the second smallest non-abelian simple group.

Example 2: $S(3, 4, 8)$

The next-simplest Steiner system, one parameter step up.

- **Points.** $X = \{1, 2, \ldots, 8\}$.
- **Block count.** $\binom{8}{3} / \binom{4}{3} = 56/4 = 14$ blocks of size 4.
- Every 3-subset of X lies in exactly one block.
- $\mathrm{Aut}\big(S(3,4,8)\big) \cong \mathrm{AGL}_3(\mathbb{F}_2)$, of order 1344, acting **3-transitively** on the 8 points.

Existence is rare. For most parameters (t, k, v) no Steiner system exists at all. The ones that do are highly constrained – that constraint is exactly what forces a large, transitive automorphism group.

Why Steiner Systems → Transitive Groups

Let $G = \mathrm{Aut}(S(t,k,v))$, the permutations of X preserving the block collection $\mathcal{B}$.

Heuristic. Any two t-subsets "look alike" inside $S(t,k,v)$: each lies in a unique block, with the rest of X playing the same role around it.

So one expects G to send any t-subset to any other – i.e. to act ***t*-transitively** on X.

For the parameter set $(t,k,v) = (5,6,12)$ this turns out to be true, and the resulting group G is also **simple**. That group is M_{12}.

The Steiner System $S(5, 6, 12)$

Fact (Witt, 1938). Up to isomorphism there is a **unique** Steiner system $S(5, 6, 12)$.

- Underlying set: $X = \{1, 2, \ldots, 12\}$.
- Blocks ("hexads"): a specific collection of 6-subsets.
- Number of blocks (from the formula on the previous slide):

$$|\mathcal{B}| = \frac{\binom{12}{5}}{\binom{6}{5}} = \frac{792}{6} = 132.$$

This $S(5, 6, 12)$ is the unique Steiner system of "Mathieu type". The next one up the ladder is $S(5, 8, 24)$ – the basis of M_{24} – and there are no others with $t \geq 4$.

Constructing the Blocks: Setup

We build the 132 hexads as a single orbit of a group from Part II.

Step 1. Identify the 12 points with the projective line

$$X \;\cong\; \mathbb{P}^1(\mathbb{F}_{11}) = \mathbb{F}_{11} \cup \{\infty\} = \{0, 1, \ldots, 10, \infty\}.$$

Step 2. Let $\mathrm{PSL}_2(\mathbb{F}_{11})$ act on X by Möbius maps $z \mapsto (az+b)/(cz+d)$, $ad-bc=1$. Order 660, acting 2-transitively on the 12 points.

Step 3. Choose the 6-subset

$$B_0 = \{\infty\} \cup \{\text{nonzero squares mod } 11\} = \{\infty, 1, 3, 4, 5, 9\}.$$

Constructing the Blocks: The Orbit

Step 4. Form the $\mathrm{PSL}_2(\mathbb{F}_{11})$-orbit of B_0:

$$\mathcal{B} := \{\, g \cdot B_0 : \ g \in \mathrm{PSL}_2(\mathbb{F}_{11}) \,\}.$$

A direct check (Witt, 1938) shows $|\,\mathrm{Stab}(B_0)| = 5$, so the orbit has size

$$|\mathcal{B}| = \frac{|\,\mathrm{PSL}_2(\mathbb{F}_{11})|}{|\,\mathrm{Stab}(B_0)|} = \frac{660}{5} = 132,$$

precisely the predicted number of hexads.

These 132 hexads are exactly the blocks of $S(5, 6, 12)$.

Two Layers of Symmetry

The construction shows two nested groups of permutations:

Group	Order	Action
$\mathrm{PSL}_2(\mathbb{F}_{11})$	660	2-transitive on $\mathbb{P}^1(\mathbb{F}_{11})$
$M_{12} := \mathrm{Aut}(S(5,6,12))$	$95\,040$	sharply 5-transitive on $\{1,\dots,12\}$

$\mathrm{PSL}_2(\mathbb{F}_{11}) \subset M_{12}$ is a proper inclusion: the quotient of orders is $95\,040/660 = 144$.

So M_{12} adds permutations beyond Möbius which still preserve the block set $\mathcal{B}$. Those extra permutations are exactly what makes M_{12} jump from 3-transitive to 5-transitive.

To make "k-transitive" precise, we need a single definition.

k-Transitivity

Let G act on a set X with $|X| = n$.

Definition. G acts **k-transitively** on X if for any two ordered k-tuples of distinct points

$$(x_1, \ldots, x_k) \quad \text{and} \quad (y_1, \ldots, y_k)$$

there exists $g \in G$ such that $g(x_i) = y_i$ for all $i = 1, \ldots, k$.

In words: G "can carry any k-tuple to any other k-tuple".

- **1-transitive** = transitive (one orbit).
- **2-transitive** $\Longrightarrow$ transitive on **pairs** of distinct points.
- **k-transitive** $\Longrightarrow$ $(k-1)$-transitive (forget the last coordinate).

How Restrictive Is k-Transitivity?

If G is k-transitive on n points, the orbit of any k-tuple of distinct points has size $n(n-1)\cdots(n-k+1)$. By orbit–stabilizer:

$$|G| \;\geq\; n(n-1)(n-2)\cdots(n-k+1).$$

Examples.

- S_n is n-transitive: $|S_n| = n!$.
- A_n is $(n-2)$-transitive (any 3-cycle moves any pair into any pair, etc.).

Theorem (Jordan, completed using CFSG). For $n \geq 6$, the only 5-transitive groups on n points are

$$\boxed{S_n, \quad A_{n+2}, \quad M_{12}\ (n=12), \quad M_{24}\ (n=24).}$$

Outside the obvious S_n, A_{n+2} tower, **only two** 5-transitive groups exist in all of finite group theory.

Back to M_{12}: Order

Fact. M_{12} acts 5-transitively on $\{1, \ldots, 12\}$, and the stabilizer of any 5-tuple of distinct points is trivial.

Therefore the orbit of one 5-tuple has size $|M_{12}|$, and equals the total number of ordered 5-tuples of distinct points:

$$|M_{12}| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 = 95\,040.$$

So M_{12} achieves the lower bound from the previous slide **with equality**. That is the strongest form of 5-transitivity possible: M_{12} is **sharply 5-transitive**.

M_{11} Lives Inside

The pointwise stabilizer of one point is

$$M_{11} := \mathrm{Stab}_{M_{12}}(12) \leq M_{12}.$$

By orbit–stabilizer:

$$|M_{11}| = \frac{|M_{12}|}{12} = \frac{95\,040}{12} = 7920.$$

M_{11} acts 4-transitively on $\{1, \ldots, 11\}$.

The same theorem (now 4-transitive case) gives an even shorter list: S_n, A_{n+2}, M_{11}, M_{12}, M_{23}, M_{24}.

What Else M_{12} Touches

- M_{12} contains two non-conjugate copies of S_6, swapped by an outer automorphism – this is **the** unique exceptional outer automorphism $\mathrm{Out}(S_6) = \mathbb{Z}/2$.
- M_{12} is closely tied to the **binary Golay code** and leads, by doubling, to M_{24}, the Leech lattice, and (much further upstream) the Monster.

Another Face: the Ternary Golay Code

So far $M_{12} = \mathrm{Aut}(S(5,6,12))$ – a permutation group on 12 points. The same group has a second concrete realisation, of "linear" type.

Ternary Golay code. There is a 6-dimensional subspace

$$\mathcal{G} \subset \mathbb{F}_3^{12}$$

(unique up to equivalence) in which every nonzero vector has at least 6 nonzero coordinates, and which is self-dual under the standard inner product on $\mathbb{F}_3^{12}$. This is the **extended ternary Golay code**.

The combinatorial rigidity of $\mathcal{G}$ is, again, the source of a large symmetry group.

$M_{12} \subset \mathrm{PGL}_6(\mathbb{F}_3)$

Theorem. The group of permutations of the 12 coordinates of $\mathbb{F}_3^{12}$ that send $\mathcal{G}$ to itself, together with sign changes preserving $\mathcal{G}$, is a central double cover

$$2.M_{12} \twoheadrightarrow M_{12},$$

with kernel $\langle -I \rangle$ inside $\mathrm{GL}(\mathcal{G})$.

Restricting the action to $\mathcal{G} \cong \mathbb{F}_3^6$ and modding out the central $\pm I$:

$$\boxed{M_{12} \subset \mathrm{PGL}_6(\mathbb{F}_3).}$$

Two faces of the same group: a 5-transitive permutation group on 12 points (combinatorial), and a small linear subgroup of $\mathrm{PGL}_6(\mathbb{F}_3)$ (algebraic).

Summary of Example 2

M_{12} is **sporadic**: not a member of any infinite family.

It exists because $S(5, 6, 12)$ exists.

After Mathieu's five sporadics in 1861, none were found for over a century – then between 1965 and 1982 the remaining 21 sporadics emerged, ending with the Monster.

Part IV

Example 3 – G_2 (exceptional Lie type), via the Octonions

Hurwitz's Theorem

Theorem (Hurwitz, 1898). Up to isomorphism, the only finite-dimensional normed division algebras over $\mathbb{R}$ are

Algebra	$\dim_{\mathbb{R}}$	Properties
$\mathbb{R}$	1	the reals
$\mathbb{C}$	2	commutative, associative
$\mathbb{H}$	4	associative, **not** commutative
$\mathbb{O}$	8	alternative, **not** associative

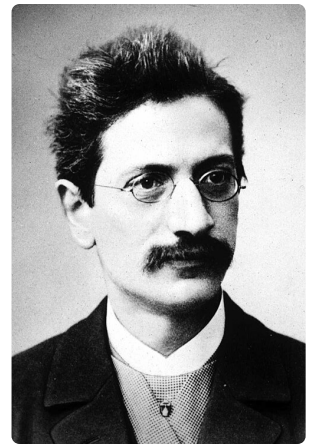
Each is built from the previous by **Cayley–Dickson doubling**, and at each step one property is lost.

Adolf Hurwitz (1859–1919)

German mathematician, student of Felix Klein, professor at ETH Zürich (1892–1919). He was a master of complex analysis, number theory, and the algebra of forms.

His **1898** paper *Über die Composition der quadratischen Formen von beliebig vielen Variabeln* showed that the multiplicative norm identity $N(xy) = N(x)N(y)$ admits real solutions only in dimensions $1, 2, 4, 8$ – the classification result behind the table above.

His name is also attached to the **Hurwitz zeta function**, the **Hurwitz quaternions**, and the **Hurwitz automorphisms theorem** (a Riemann surface of genus $g \geq 2$ has at most $84(g-1)$ automorphisms).



A. Hurwitz (1859–1919)

Cayley–Dickson Doubling

Given an algebra A with conjugation $a \mapsto \bar{a}$, define $A \oplus A$ with

$$(a, b)(c, d) := (ac - \bar{d}b,\ da + b\bar{c}),$$

$$\overline{(a, b)} := (\bar{a}, -b).$$

- $\mathbb{C} =$ doubling of $\mathbb{R}$.
- $\mathbb{H} =$ doubling of $\mathbb{C}$ – loses commutativity.
- $\mathbb{O} =$ doubling of $\mathbb{H}$ – loses associativity (keeps alternativity: $(xx)y = x(xy)$).
- Doubling once more produces the sedenions, which are **not** a division algebra. The tower stops.

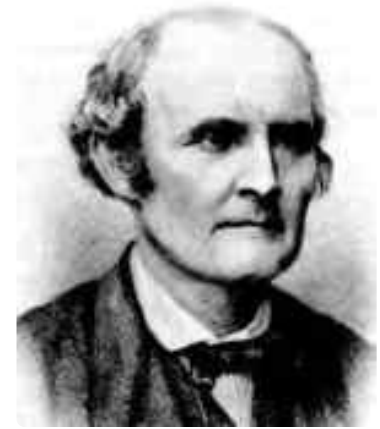
Arthur Cayley (1821–1895)

British mathematician, founding figure of group theory and matrix algebra.

He gave the first abstract definition of a group; **Cayley's theorem** states that every group embeds in some symmetric group.

In **1845** he wrote down what we now call the **octonions**, doubling Hamilton's quaternions $\mathbb{H}$ to an 8-dimensional algebra. (J. T. Graves discovered them independently a few months earlier; the systematic *doubling* recipe was generalized by L. E. Dickson, hence "Cayley–Dickson".)

Author of more than 900 papers; his name lives on in the Cayley table, Cayley graph, Cayley–Hamilton theorem, and the Cayley transform.



A. Cayley (1821–1895)

What an Octonion Looks Like

$\mathbb{O}$ has basis $1, e_1, \ldots, e_7$ over $\mathbb{R}$, with

$$e_i^2 = -1, \qquad e_i e_j = -e_j e_i \quad (i \neq j).$$

The full multiplication table is encoded by the **Fano plane** – 7 lines, each carrying a copy of imaginary quaternions.

Norm $N(x) := x\bar{x} \in \mathbb{R}$ is multiplicative:

$$N(xy) = N(x)\, N(y)$$

– the **eight-square identity**.

Tower of Automorphism Groups

Algebra	$\mathrm{Aut}(\cdot)$	$\dim$
$\mathbb{R}$	trivial	0
$\mathbb{C}$	$\mathbb{Z}/2$ (complex conjugation)	0
$\mathbb{H}$	$\mathrm{SO}(3)$ (rotations of $\mathrm{Im}\,\mathbb{H}$)	3
$\mathbb{O}$	$\boxed{G_2}$	14

Each step up the algebra tower, the automorphism group jumps in dimension.

$$\boxed{G_2 := \mathrm{Aut}(\mathbb{O}).}$$

Why G_2 Is "Exceptional"

Theorem (Cartan, 1894). Simple Lie algebras over $\mathbb{C}$ split into

- four classical infinite families: A_n, B_n, C_n, D_n;
- five **exceptional** Lie algebras: G_2, F_4, E_6, E_7, E_8.

G_2 is the smallest exceptional one. "Exceptional" means: not in any infinite family, in the same spirit as $M_{11}, \ldots, M_{24}$ are sporadic.

And $G_2 = \mathrm{Aut}(\mathbb{O})$ gives a beautifully concrete model.

Élie Cartan (1869–1951)

É. Cartan (1869–1951)

French mathematician; one of the founders of modern differential geometry and the theory of Lie groups.

His **1894 thesis** *Sur la structure des groupes de transformations finis et continus* completed the classification of complex simple Lie algebras: four classical infinite families A_n, B_n, C_n, D_n and **five** exceptional ones G_2, F_4, E_6, E_7, E_8.

Cartan also pioneered the theory of **spinors**, **exterior differential forms** and **moving frames** in differential geometry. His son Henri Cartan became one of the founders of Bourbaki and a leading algebraic topologist.

G_2 over $\mathbb{F}_p$

The same definition works over any field.

For p prime, define $\mathbb{O}_{\mathbb{F}_p}$ – the (split) octonion algebra over $\mathbb{F}_p$ – by Cayley–Dickson doubling, replacing $\mathbb{R}$ with $\mathbb{F}_p$.

$$G_2(\mathbb{F}_p) := \mathrm{Aut}\big(\mathbb{O}_{\mathbb{F}_p}\big).$$

$$\boxed{|G_2(\mathbb{F}_p)| = p^6\,(p^6-1)(p^2-1).}$$

(For prime-power $q = p^k$, replace p by q. Building $\mathbb{F}_q$ needs Galois theory, so today we keep p prime.)

Simplicity over $\mathbb{F}_p$

Theorem (Dickson, 1905). $G_2(\mathbb{F}_p)$ is simple for every prime $p \geq 3$.

Exception. $G_2(\mathbb{F}_2)$ has order $12\,096 = 2 \cdot 6048$ and is **not** simple.

Its derived subgroup is

$$G_2(\mathbb{F}_2)' \cong \mathrm{PSU}_3(\mathbb{F}_3),$$

a classical Lie type group of order 6048.

Same flavour as $\mathrm{PSL}_2(\mathbb{F}_2) \cong S_3$ and $\mathrm{PSL}_2(\mathbb{F}_3) \cong A_4$ – small characteristic spoils simplicity.

Smallest Examples

p	$\lvert G_2(\mathbb{F}_p)\rvert$	simple?
2	$12\,096$	no (derived $\cong \mathrm{PSU}_3(\mathbb{F}_3)$, order 6048)
3	$4\,245\,696$	**yes** – smallest simple G_2
5	$5\,859\,000\,000$	yes
7	$\approx 6.64 \times 10^{11}$	yes
11	$\approx 3.77 \times 10^{14}$	yes

For each prime $p \geq 3$: a brand-new finite simple group of **exceptional Lie type**.

Summary of Example 3

G_2 wears two faces, both captured by one definition:

$$\boxed{G_2 = \mathrm{Aut}(\mathbb{O}).}$$

- Over $\mathbb{R}$: a 14-dim simple Lie group, exceptional.
- Over $\mathbb{F}_p$ (prime $p \geq 3$): a finite simple group, of exceptional Lie type – parallel to but distinct from $\mathrm{PSL}_n(\mathbb{F}_p)$.

Part V

Looking Back

CFSG as a Tree

```
Finite simple groups
  |
  +-- cyclic Z_p
  |
  +-- alternating A_n   (n ⩾ 5)
  |
  +-- Lie type
  |     +-- classical:    PSL, PSU, PSp, P-Omega over finite fields
  |     +-- exceptional:  G_2, F_4, E_6, E_7, E_8 + twisted
  |
  +-- 26 sporadic
        +-- Mathieu:  M_11, M_12, M_22, M_23, M_24
        +-- 20 more (1965-1982)
        +-- Monster   (~ 8 x 10^53)
```

Today's three examples sit on three different branches: $\mathrm{PSL}_n(\mathbb{F}_p)$ on classical Lie, $G_2(\mathbb{F}_p)$ on exceptional Lie, M_{12} on sporadic. Together with $\mathbb{Z}_p$ (L01) and A_n (L04), we have now met an example from every branch.

What the Three Examples Reveal

The classification has very different textures inside each family.

- **Classical Lie (PSL_n).** A clean infinite family with a uniform construction (linear algebra) and a single small-characteristic defect.
- **Sporadic (M_{12}).** A handful of isolated groups built from rare combinatorial objects – there is no infinite family, and no construction that "explains them all".
- **Exceptional Lie (G_2).** Still an infinite family in p, but built from a non-associative algebra rather than from $\mathbb{F}_p^n$. A different algebraic phenomenon than PSL.

CFSG is the statement that **these three textures, plus $\mathbb{Z}_p$ and A_n, exhaust everything.**

Bridges to Coming Chapters

Bridge 1 — division rings. Octonions are the last normed division algebra. Ring theory begins with division rings.

Bridge 2 — Galois of finite fields. $G_2(\mathbb{F}_q)$ for $q = p^k$ uses $\mathbb{F}_q$, whose construction is one of the first applications of Galois theory. Its Galois group is cyclic, generated by the Frobenius.

References — CFSG and Sporadic Groups

- **Aschbacher, M.** *Finite Group Theory*. Cambridge Univ. Press, 2nd ed., 2000. — Standard reference for the structural side of CFSG.
- **Conway, J. H.; Sloane, N. J. A.** *Sphere Packings, Lattices and Groups*. Springer, 3rd ed., 1999. Ch. 10–11. — The Mathieu groups, $S(5,6,12)$, $S(5,8,24)$, the Golay code, the Leech lattice.
- **Wilson, R. A.** *The Finite Simple Groups*. Graduate Texts in Math. 251, Springer, 2009. — Modern textbook covering all four families with explicit constructions.
- **Solomon, R.** "A brief history of the classification of the finite simple groups." *Bull. Amer. Math. Soc.* 38 (2001), 315–352. — Historical overview of the CFSG project.
- **ATLAS of Finite Groups** (Conway, Curtis, Norton, Parker, Wilson, 1985). — Character tables, presentations, maximal subgroups for sporadic and small groups.

References — Exceptional Groups

- **Hurwitz, A.** "Über die Composition der quadratischen Formen von beliebig vielen Variabeln." *Nachr. Ges. Wiss. Göttingen* (1898), 309–316. — Classification of normed division algebras.
- **Cartan, É.** "Sur la structure des groupes de transformations finis et continus." Thèse, Paris, 1894. — Classification of complex simple Lie algebras, including G_2, F_4, E_6, E_7, E_8.
- **Dickson, L. E.** "A new system of simple groups." *Math. Ann.* 60 (1905), 137–150. — Construction and simplicity of $G_2(\mathbb{F}_q)$.
- **Springer, T. A.; Veldkamp, F. D.** *Octonions, Jordan Algebras and Exceptional Groups*. Springer Monographs, 2000. — $\mathbb{O}$, G_2, F_4, and the rest of the exceptional family.
- **Baez, J. C.** "The octonions." *Bull. Amer. Math. Soc.* 39 (2002), 145–205. — Highly readable survey: $\mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$ and the exceptional Lie algebras.

What to Remember

1. CFSG: every finite simple group is cyclic of prime order, alternating ($n \geq 5$), Lie type (classical or exceptional), or one of 26 sporadic.
2. $\mathrm{PSL}_n(\mathbb{F}_p)$ – classical Lie, infinite family, simple except for $(n, p) = (2, 2), (2, 3)$.
3. $M_{12} = \mathrm{Aut}(S(5, 6, 12))$ – sporadic, 5-transitive on 12 points, of order $95\,040$. Blocks built as one $\mathrm{PSL}_2(\mathbb{F}_{11})$-orbit.
4. $G_2 := \mathrm{Aut}(\mathbb{O})$, with finite version $G_2(\mathbb{F}_p)$ of order $p^6(p^6 - 1)(p^2 - 1)$ – exceptional Lie, simple for $p \geq 3$.

Homework (Lecture 9)

Problem 1. Mathieu and stabilizers.

Let G act k-transitively on n points ($k \geq 1,\ n \geq k$).

a. Show that the stabilizer of any one point is $(k-1)$-transitive on the remaining $n-1$ points.

b. Use 5-transitivity of M_{12} on $\{1, \ldots, 12\}$ to conclude $|M_{11}| = 7920$.

Homework (Lecture 9)

Problem 2. Octonion automorphisms.

Let $\varphi : \mathbb{O} \to \mathbb{O}$ be an $\mathbb{R}$-algebra automorphism.

a. Show that $\varphi(1) = 1$.

b. Show that φ commutes with conjugation: $\varphi(\bar{x}) = \overline{\varphi(x)}$.

c. Show that φ preserves the norm $N(x) = x\bar{x}$.

d. Conclude that φ restricts to an element of $\mathrm{O}(7)$ on $\mathrm{Im}\,\mathbb{O}$, so $G_2 \subseteq \mathrm{O}(7)$.

Homework (Lecture 9)

Problem 3. G_2 over $\mathbb{F}_p$.

a. From the formula $|G_2(\mathbb{F}_p)| = p^6(p^6-1)(p^2-1)$, compute

$$|G_2(\mathbb{F}_3)| \quad \text{and} \quad |G_2(\mathbb{F}_5)|.$$

b. Verify $|G_2(\mathbb{F}_2)| = 12\,096$ and check that $12\,096 = 2 \cdot 6048$ with $6048 = |\mathrm{PSU}_3(\mathbb{F}_3)|$.

Questions?